

3,690 views | Jul 24, 2019, 9:49 am

NSA Launches Cybersecurity Arm To Defend The U.S. From Foreign Adversaries

Kate O'Flaherty Senior Contributor ⓘ

[Cybersecurity](#)

I'm a cybersecurity journalist.



The NSA has announced the launch of a cybersecurity directorate to help to defend against foreign adversaries. Is it a good idea? Photocredit: PAUL J. RICHARDS/AFP /Getty Images GETTY

The National Security Agency (NSA) has announced its intention to create a cybersecurity directorate this fall in a bid to defend the U.S. against foreign adversaries. It comes at a time of increasing election interference by [foreign nations such as Russia](#) as part of [an ongoing strategy to destabilize the West](#).

defensive operations. The [NSA said via Twitter](#): “Start spreading the news, #NSA is operationalizing intelligence to secure the country.”

It is expected the NSA’s cybersecurity directorate, which will become operational on October 1, will be headed up by Anne Neuberger who already has a lead role at the U.S. intelligence agency.

The latest move by the NSA coincides with a broader fusion of the intelligence agency’s offensive and defensive portfolios, the *Wall Street Journal* said. This has been taking place for several years and expanded under U.S. Cyber Command and NSA chief General Paul Nakasone.

Nakasone announced the new cybersecurity directorate on July 23 at the International Conference on Cyber Security at Fordham University. “Over the past couple years, as we did a number of different reorganizations, one of the things I think we lost was that emphasis on cybersecurity,” he said.

NSA cybersecurity directorate’s mission

It comes at a time of increasing focus on cybersecurity by the U.S. government. In early July, [it announced a surprising move to secure power grids by using “retro” technologies](#). This followed numerous attempts by foreign actors to launch cyberattacks on so-called critical national infrastructure (CNI).

Under President Donald Trump, the NSA has been engaging in a more aggressive strategy to defend against foreign adversaries such as China, Russia, Iran and North Korea (CRINK). Led offensively by the Cyber Command and supported by the NSA’s intelligence collecting, these efforts have predominantly focused on stopping election interference. It comes after Russia was accused of interfering with the 2016 U.S election—an allegation which it denies.

against foreign adversaries.

Much like the U.K.'s GCHQ cybersecurity arm, the National Cyber Security Center (NCSC), the NSA's cybersecurity directorate will aim to protect the U.S. from foreign adversaries by sharing more information with other federal agencies and the private sector.

NSA cybersecurity directorate: A good idea?

At a time of increasing cyberattacks and election interference, is this new unit a good idea? Philip Ingram MBE, a former colonel in British military intelligence thinks so. He points out that military unit the U.S. Cyber Command has existed for “quite some years.” This unit has a defense remit, as well as an attack remit and capability, he says.

He says the cybersecurity directorate could be the NSA on a mission to grab funding. “There is always a competition between agencies for intelligence funding and I suspect after Trump's Russian interference debacle, there have been a few ‘rollockings’ flying around—and more money on offer.”

In addition, says Ingram: “They have been looking at the U.K.'s NCSC with some envy and are copying the model—which can only be a good thing.”

Its capabilities can not be doubted. The NSA has been directly involved in supporting military operations overseas and represents “the most sophisticated set of signals intelligence capabilities found in the world today,” Ian Thornton-Trump, security head at AMTrust Europe says.

However, some experts question what is effectively giving the NSA more responsibility, [given allegations about spying](#) and the [Edward Snowden revelations](#). Thornton-Trump, points out that having a military or government organization assume responsibility for defense of the public internet “might be a bit disconcerting for many folks.”

says. “It is a very difficult position to be in without appropriate governance and oversight which may not necessarily be in place given a new domestic mandate.”

This latest move comes as [Attorney General William P. Barr defended](#) the use of encryption backdoors—which most security experts agree would be a huge disaster.



Kate O'Flaherty Senior Contributor

I'm a freelance cybersecurity journalist with over a decade's experience reporting on the issues impacting users, businesses and the public sector. My interests within... **Read More**

Forbes

© 2019 Forbes Media LLC. All Rights Reserved.

[AdChoices](#) | [Privacy Statement](#) | [Terms and Conditions](#) | [Contact Us](#) | [Jobs At Forbes](#) |
[Reprints & Permissions](#) | [Forbes Press Room](#) | [Advertise](#)